

FILED

AO 104.00650 (10) Application for a Search Warrant (Modified: WAWD 10-26-18)

APR 29 2019

UNITED STATES DISTRICT COURT

CERTIFIED TRUE COPY
ATTEST: WILLIAM M. MCCOOL
Clerk, U.S. District Court
Western District of WashingtonAT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
BY

for the

Western District of Washington

Deputy Clerk

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)Information associated with safirion@outlook.com
and other email accounts that are stored at premises
controlled by Microsoft Corp.

Case No.

MJ19-177

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, incorporated herein by reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 1341, 1343,
1956(a)(1) and 1957

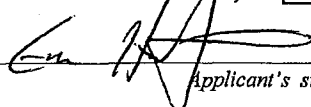
Offense Description

Mail fraud, wire fraud, money laundering

The application is based on these facts:

- ☒ See Affidavit of Special Agent Eric Hergert, continued on the attached sheet.

- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☐ by reliable electronic means; or: ☐ telephonically recorded.

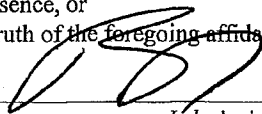
Applicant's signature

Eric Hergert, Special Agent

Printed name and title

- ☒ The foregoing affidavit was sworn to before me and signed in my presence, or
- ☐ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 04/29/2019



Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, Chief United States Magistrate Judge

Printed name and title

STATE OF WASHINGTON)
)
COUNTY OF KING) SS

I, Eric Hergert, being first duly sworn, depose and state as follows:

1. I am a Special Agent with Internal Revenue Service, Criminal Investigation (IRS-CI), and have been so employed since September 2009. I am presently assigned to IRS-CI's Western Area Cyber Crime Unit in the Los Angeles Field Office. My duties and responsibilities include the investigation of possible criminal violations of the Internal Revenue laws (Title 26, United States Code), the Bank Secrecy Act (Title 31, United States Code), the Money Laundering Control Act of 1986 (Title 18, United States Code, Sections 1956 and 1957), and other related offenses.

2. I earned a Bachelor of Arts degree in accounting from the University of Washington, Tacoma, in 2002. I attended the Criminal Investigator Training Program and the IRS Special Agent Basic Training at the Federal Law Enforcement Training Center (FLETC) where I received detailed training in conducting financial investigations. The training included search and seizure, the Internal Revenue laws, and IRS procedures and policies in criminal investigations. I have also attended various cybercrime and virtual currency related trainings, including at FLETC and others. Before being hired by IRS-CI, I was employed as a Revenue Agent for the IRS for approximately five years, performing civil examinations of small businesses and self-employed individuals. As a Revenue Agent, I received approximately 16 weeks of specialized training in personal, partnership, and corporate income tax, as specified in the Internal Revenue Code.

3. I have conducted and assisted in several investigations involving financial crimes. I have led and participated in the execution of search warrants and have

1 interviewed witnesses and defendants who were involved in, or had knowledge of,
2 violations of the Internal Revenue Code, the Bank Secrecy Act, and the Money
3 Laundering Control Act. In the course of my employment with IRS-CI, I have conducted
4 and have been involved in investigations of alleged criminal violations, which have
5 included tax evasion (26 U.S.C. § 7201), filing a false tax return (26 U.S.C. § 7206(1)),
6 aiding or assisting in the preparation of false tax returns (26 U.S.C. § 7206(2)),
7 conspiring to defraud the United States (18 U.S.C. § 371), wire and mail fraud (18 U.S.C.
8 §§ 1343, 1341), aggravated identity theft (18 U.S.C. § 1028A), and money laundering (18
9 U.S.C. §§ 1956, 1957), among others.

10 4. I have led and participated in the execution of federal search warrants and
11 the consensual searches of records relating to the concealment of assets and proceeds
12 derived from fraud. These records included, but were not limited to, email accounts,
13 instant messages, personal telephone books, photographs, bank records, escrow records,
14 credit card records, tax returns, business books and records, and computer hardware and
15 software.

16 5. I also have specialized training in cryptocurrencies, with a focus on Bitcoin
17 and Ethereum. This has included training into how publically viewable "blockchains"
18 record cryptocurrency transactions, how to trace funds through these transactions,
19 attribution techniques used to identify individuals responsible for conducting the
20 transactions, and methods used by individuals to obfuscate the source or their control of
21 cryptocurrencies. I have used these techniques in prior and ongoing investigations.
22 Additionally, I have conducted cryptocurrency training for others, both internal to the
23 IRS, as well as for external third parties.

24 6. The facts set forth in this Affidavit are based on my own personal
25 knowledge; knowledge obtained from other individuals during my participation in this
26 investigation, including other law enforcement officers; review of documents and records
27 related to this investigation; communications with others who have personal knowledge
28

AFFIDAVIT OF SA HERGERT
USAO#2018R01443

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE
5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

1 of the events and circumstances described herein; and information gained through my
2 training and experience.

3 7. This affidavit does not detail each and every fact and circumstance I or
4 others have learned during the course of this investigation. Furthermore, the
5 investigation is ongoing, including the gathering and analysis of records. I have set forth
6 only the facts that I believe are necessary to establish probable cause to believe that
7 evidence, fruits and instrumentalities of Mail Fraud, in violation of Title 18, United States
8 Code, Section 1341, Wire Fraud, in violation of Title 18, United States Code, Section
9 1343, and Money Laundering, in violation of Title 18, United States Code, Sections
10 1956(a)(1) and 1957, will be found on the SUBJECT EMAIL ACCOUNTS.

11 **SUMMARY OF THE FRAUDULENT SCHEME**

12 8. The target of this investigation is VOLODYMYR KVASHUK. The
13 investigation has shown that KVASHUK devised and executed a scheme to defraud
14 Microsoft Corporation ("Microsoft"). KVASHUK worked for Microsoft and was
15 assigned to test the company's online retail sales platform. In that role, KVASHUK was
16 supposed to make simulated purchases of Microsoft products from the company's online
17 store. The testing system was designed to ensure that no physical products would be
18 shipped. KVASHUK, however, used his testing account to purchase massive amounts of
19 "currency stored value," or "CSV," such as digital gift cards. The testing program was
20 not supposed to involve purchases of CSV, and no mechanisms were in place to prevent
21 the delivery of valuable CSV to the tester. The investigation has shown that KVASHUK,
22 in his role as a tester, purchased millions of dollars of CSV, which he then resold on the
23 Internet. KVASHUK used the proceeds of the fraud to purchase, among other things, a
24 \$160,000 Tesla car and a \$1.6 million home in Renton.

25 9. Email was central to KVASHUK's scheme. The testing program involved
26 the creation and use of email accounts for the sole purpose of making simulated
27 purchases. KVASHUK used a variety of email accounts to make unauthorized purchases
28 of CSV, and also to purchase goods from Microsoft with the stolen CSV.

AFFIDAVIT OF SA HERGERT
USAO#2018R01443

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE
5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

PLACES TO BE SEARCHED AND ITEMS TO BE SEIZED

10. This affidavit is being submitted in support of an application for warrants authorizing the search of the following email accounts (collectively referred to as the "SUBJECT EMAIL ACCOUNTS"):

- a. safirion@outlook.com;
- b. kvashuk.volodymyr@gmail.com;
- c. [REDACTED]@outlook.com;
- d. [REDACTED]@outlook.com;
- e. mstest_v-vokvas@outlook.com; and
- f. [REDACTED]@outlook.com.

11. The information associated with the safirion@outlook.com, [REDACTED]@outlook.com, [REDACTED]@outlook.com, [REDACTED]@outlook.com, and [REDACTED]@outlook.com email accounts is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, an e-mail provider headquartered at 1 Microsoft Way, Redmond, Washington 98052, as further described in Attachment A, attached hereto and incorporated herein. The information associated with the kvashuk.volodymyr@gmail.com email account is stored at premises owned, maintained, controlled, or operated by Google Incorporated, an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043, as further described in Attachment A-1, attached hereto and incorporated herein. Google and Microsoft are collectively referred to as the "Providers."

12. The information to be searched is described in the following paragraphs and in Attachments B and B-1. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the Providers to disclose to the government copies of the information (including the content of communications) further described at Attachments B and B-1. Upon receipt of the information described in Section I of Attachments B and B-1, government-authorized persons will review that information to locate the items described in Section II

AFFIDAVIT OF SA HERGERT
USAO#2018R01443

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE
5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

1 of the Attachments. A preservation request for the relevant account was served on
2 Google on February 1, 2019, and this warrant seeks all responsive material preserved
3 pursuant to that request (Google reference number 2307267).

4 **SUMMARY OF THE INVESTIGATION**

5 13. As part of this investigation, I have obtained records from numerous
6 sources, met with counsel for Microsoft, and interviewed Microsoft employees who
7 investigated the CSV theft.

8 **Microsoft's Program To Test Online Retail Sales**

9 14. Microsoft has given me a copy of VOLODYMYR KVASHUK's resume,
10 which shows that he is a Seattle-based software engineer. According to information
11 provided by Microsoft, KVASHUK was an employee of a Microsoft vendor. As part of
12 his employment with the vendor, KVASHUK worked for Microsoft from August 26,
13 2016, until October 1, 2017. During that time, KVASHUK worked out of Microsoft's
14 office and had access to the company's computer network. On December 1, 2017,
15 Microsoft hired KVASHUK as a full-time employee with an annual salary of
16 approximately \$116,000. KVASHUK worked for Microsoft until June 22, 2018.

17 15. Microsoft sells various products to the general public over the Internet via
18 its online store. To make purchases from the Microsoft store, a customer must establish a
19 Microsoft store account that is linked to an email address and to one or more payment
20 devices (such as a credit card). As both an employee of an outside vendor, and as a
21 Microsoft employee, KVASHUK was a member of Microsoft's Universal Store Team
22 ("UST"), which supports the company's online retail platform, by (among other things)
23 managing a program that tests the online sales system. The testing program involves
24 creating test accounts that are linked to test email accounts created specifically for the
25 purpose of the testing program. A tester creates a test email account by using a naming
26 convention for the account: the name begins with "mstest," followed by an underscore
27 and the user name of the tester. The tester then requests that the UST team "whitelist"
28 the account, meaning that purchases made from the account will automatically bypass

AFFIDAVIT OF SA HERGERT
USAO#2018R01443

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE
5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

1 Microsoft's security and risk protocols, which monitor online purchases in order to detect
2 possible fraud. The test accounts are linked to artificial payment devices ("Test in
3 Production" or "TIP" cards) – in effect, phony credit cards – that allow the tester to
4 simulate a purchase without generating an actual charge. Once the whitelisted account
5 was created, the tester would use that account to attempt to make online product
6 purchases from Microsoft, just as an ordinary consumer would. Although in theory each
7 test account was supposed to be used by the tester who created the account, in reality, the
8 login and password information for the test accounts was stored in an electronic
9 document that was accessible to multiple testers.

10 16. According to Microsoft, the testing program was designed to test the
11 company's online sales of physical goods only. When a tester used a whitelisted account
12 to purchase physical goods, the system ensured that no goods were actually delivered.

13 17. According to Microsoft, the testing program was not designed for simulated
14 purchases of electronic currency stored value ("CSV"), such as digital gift cards. Testers
15 were not authorized to use test accounts to make test purchases of CSV. Because
16 Microsoft did not expect testers to purchase CSV, the system had no safeguards to
17 prevent the delivery of actual, usable CSV to a tester who made a purchase from a
18 whitelisted account. Accordingly, if a tester did purchase CSV, the system would
19 generate and deliver a valid and usable product "key" that could be "redeemed," meaning
20 that the value of the digital currency would be added to an electronic "wallet" linked to a
21 customer account. Once redeemed, the CSV could be used to buy both physical and
22 digital products from the Microsoft store.

23 The Theft Of \$10 Million In Microsoft's Digital Currency

24 18. According to information provided by Microsoft, in February of 2018,
25 Microsoft's UST Fraud Investigation Strike Team ("FIST") noticed a suspicious increase
26 in the use of CSV to buy subscriptions to Microsoft's Xbox live gaming system from
27 Microsoft's online store. FIST investigated and discovered that the suspicious CSV had
28 originally been purchased from Microsoft through two whitelisted test accounts

1 associated with the email accounts [REDACTED]@outlook.com and
2 [REDACTED]@outlook.com (the '[REDACTED]' and '[REDACTED]' test accounts). The
3 CSV was then resold on the secondary market, at a steep discount, via at least two online
4 reseller websites, g2a.com and nokeys.com. Customers who purchased the CSV on the
5 secondary market then redeemed the CSV at Microsoft's online store for Xbox live
6 subscriptions.

7 19. The websites g2a.com and nokeys.com are located at IP addresses
8 88.198.39.152 and 67.229.64.252, respectively. According to open source research, the
9 servers hosting these websites are located in Germany and California, respectively. All
10 transmissions of CSV information to be sold through these websites are communication
11 by wire through interstate or foreign commerce if those transmissions originate in
12 Washington state. The [REDACTED] and [REDACTED] test accounts were not established by
13 KVASHUK, but rather by other Microsoft employees. However, the username and
14 passwords for those and other test accounts were stored on Microsoft's network, giving
15 KVASHUK and many other Microsoft employees access to them. FIST discovered that
16 the [REDACTED] and [REDACTED] test accounts were used to buy a large amount of CSV
17 between November 2017 and March 2018. The [REDACTED] and [REDACTED] accounts were
18 blocked by Microsoft on or about March 15, 2018. FIST later discovered that a third test
19 account linked to [REDACTED]@outlook.com (the "[REDACTED]" test account) was also
20 responsible for a suspicious spike in CSV purchases, conducting approximately 166
21 purchases of CSV between March 22 and March 23, 2018. This account was blocked on
22 or about March 23, 2018.

23 20. The three suspicious test accounts were used to purchase roughly \$10
24 million in CSV from Microsoft. Microsoft was able to "blacklist" roughly \$1.8 million in
25 CSV to prevent it from being redeemed, resulting in a total loss to Microsoft of over \$8.2
26 million.

27 21. Microsoft interviewed the employees who created the three suspicious test
28 accounts and found no evidence that they were involved in the fraudulent CSV purchases.

1 Evidence Of Kvashuk's Involvement In The Theft

2 22. A variety of evidence shows that KVASHUK was involved in the CSV
3 theft from Microsoft.

4 *Kvashuk's Use Of His Own Test Account For Theft*

5 23. As an initial matter, KVASHUK has admitted to Microsoft investigators
6 using the Microsoft store test account that he created – linked to mstest_v-
7 vokvas@outlook.com (the “vokvas” test account”) – to make unauthorized purchases.
8 Microsoft records show that the vokvas test account made purchases (typically of CSV)
9 on April 28, July 10, September 29, October 4, October 7, October 11, and October 22 of
10 2017. The amount of CSV purchased through the vokvas account was relatively small,
11 and not all of the CSV was redeemed.

12 24. On October 7, 2017, the vokvas test account was used to purchase an
13 electronic “token” for a subscription to Microsoft Office. That token was redeemed by a
14 Microsoft store account linked to the email address admin@searchdom.io (the
15 “searchdom” account). Microsoft records show that the name on the “searchdom”
16 account is “Volo kvashuk,” and the address is an apartment complex, 5035 15th Avenue,
17 Unit 101, in Seattle (the “15th Avenue” apartments). A copy of KVASHUK’s resume
18 (provided by Microsoft) lists him as the co-founder and Chief Technology Officer of
19 “SearchDom.”

20 25. According to Microsoft records, KVASHUK’s vokvas test account was
21 used to purchase approximately \$10,164.99 in CSV in October 2017. On October 22 and
22 24, 2017, approximately \$2,500 in CSV obtained by the vokvas test account was
23 redeemed to Microsoft store accounts linked to the email addresses
24 pikimajado@tinoza.org (the “pikimajado” account) and xidijenizo@axsup.net (the
25 “xidijenizo” account). On October 22 and 24, 2017, the redeemed CSV in the
26 pikimajado and xidijenizo accounts were used to order three video or “graphics” cards
27
28

1 with a total cost of approximately \$2,024.58 from Microsoft's online store.¹ Microsoft's
2 records show that the name and address associated with the pikimajado and xidijenizo
3 accounts is "Grigor shikor" at the same 15th Avenue apartment complex that KVASHUK
4 lived at, but at Unit 309 (instead of KVASHUK's unit, 101). Microsoft provided the
5 FedEx tracking numbers for the shipment of these cards. By entering the tracking
6 numbers into FedEx's website, I was able to determine the video cards were shipped
7 from Ontario, California to Seattle, Washington on or about October 22nd and 24th of
8 2017. Additionally, FedEx's website indicated that at least one of the video cards was
9 delivered to the recipient address. From my training and experience, I know that FedEx
10 is a "private or commercial interstate carrier" as that term is used in Title 18, United
11 States Code, Section 1341.

12 26. As part of my investigation, I obtained phone records for 951-397-8122,
13 which is listed as KVASHUK's phone on his resume. The subscriber name on that
14 account is "Grigory" KVASHUK. Public records searches by Microsoft revealed no
15 "Grigor shikor" in Washington.

16 27. According to Microsoft records, approximately \$600 of the CSV purchased
17 by the vokvas account was redeemed to a Microsoft store account linked to the email
18 address safirion@outlook.com (the "safirion" account). According to Microsoft, the
19 name on the account is "volo kv". The current address was on 7th Avenue in Seattle, and
20 the former address was KVASHUK's apartment at the 15th Avenue complex.

21 28. Microsoft investigators interviewed KVASHUK on May 10 and May 18 of
22 2018. Although no law enforcement officer was at those interviews, I have listened to
23 recordings of the interviews. The interviews were not completely recorded because of a
24 technical problem, but I have also read summaries of the interviews and spoken with
25
26

27 ¹ Microsoft records show attempts to access the vokvas test account from IP addresses located in Russian and Japan
28 on October 22, 2017. These may have been attempts by KVASHUK to disguise his IP address, although that has
not been confirmed.

1 Andy Cookson of Microsoft, who was present at both interviews. The interviewers asked
2 KVASHUK about the purchases made with the vokvas test account.

3 29. KVASHUK admitted that he had created the vokvas account. He also
4 admitted to making some unauthorized purchases from the account. KVASHUK
5 suggested that there was a lack of guidance from his superiors about what could and
6 could not be purchased via a test account, and claimed to have only been told that test
7 accounts should not be used to purchase subscriptions. KVASHUK claimed that he
8 believed it was permissible to use test accounts to buy CSV because it was not "real"
9 money.

10 30. KVASHUK admitted to Microsoft investigators that he used his test
11 account to purchase CSV. He admitted that the "safirion" account was his personal
12 account, and that he used stolen CSV to buy movies from the Microsoft store.
13 KVASHUK admitted that he had tried to buy a video card, but claimed that it had never
14 arrived.

15 31. The investigators asked KVASHUK about the video cards purchased (using
16 CSV obtained by the vokvas test account) in the name of "Grigor shikor" at Unit 309 of
17 the 15th Avenue complex. KVASHUK denied purchasing those cards. When asked if he
18 knew "Grigor shikor," KVASHUK initially said, "it's complicated," but then denied
19 knowing him.² KVASHUK admitted that he lived at the 15th Avenue complex, but
20 denied receiving the cards.

21 32. With respect to the Office subscription purchased by the searchdom
22 account (using a token obtained by the vokvas test account), KVASHUK said that he and
23 another person were business partners in SearchDom. KVASHUK said that he did not
24 remember this event and suggested that he might have made a mistake.

25
26
27
28 ² This part of the interview was not recorded.

Evidence Linking KVASHUK To CSV Thefts Through Other Test Accounts.

33. The vast majority of the \$10 million in stolen CSV was obtained through the avestu, sfwe2eauto, and zabeerj2 test accounts. As noted, although these accounts were created by other testers, KVASHUK would have had access to the login information necessary to access these accounts. Based on information provided by Microsoft, it appears that these accounts were used to make unauthorized CSV purchases from approximately November 26, 2017, through March 23, 2018.³ As best as can be determined from the available information, it appears that CSV was resold (most likely at a steep discount) through online resellers, to customers who used the CSV to make purchases from Microsoft's online store.

34. Although KVASHUK admitted to only making very limited purchases of CSV from his test account, the investigation has shown probable cause to believe that KVASHUK used the [REDACTED], [REDACTED], and [REDACTED] accounts to make unauthorized CSV purchases. Some of the evidence comes in the form of Internet Protocol ("IP") address data. An IP address is a numerical label assigned to each device that is connected to a computer network that accesses the Internet. In general, Microsoft's online sales platform records the IP addresses used to access the company's website. However, because the test accounts bypassed several safeguards, IP addresses were only captured on approximately 489 of 1,554 transactions.

35. Microsoft records show that between December 29, 2017 and March 23, 2018, at least \$2.4 million of CSV was purchased using the [REDACTED], [REDACTED] and [REDACTED] accounts in over 400 transactions from devices using at least 34 different IP addresses beginning with 173.244.44, including IP addresses 173.244.44.19 (February 2018 and March 2018), 173.244.44.37 (December 2017 and March 2018), 173.244.44.58 (February 2018 and March 2018), and 173.244.44.89 (January 2018, February 2018, and

³ KVASHUK was not employed at Microsoft for the early part of this time period, but could have used any Internet-enabled device to access and log into the accounts.

1 March 2018). According to Microsoft, numerous Microsoft employees have logged in
2 via these addresses, leading them to believe the IP addresses are publically accessible.

3 36. The investigation has shown that KVASHUK used a 173.244.44 IP address
4 to access a Microsoft store account linked to his personal email address,
5 kvashuk.volodymyr@gmail.com (the "kvashuk" account)⁴ at least nine times in
6 December 2017, including IP addresses 173.244.44.19, 173.244.44.37, and
7 173.244.44.58. He also logged into his Coinbase cryptocurrency account using IP
8 address 173.244.44.89 on December 2, 2017. However, no incidents have been identified
9 where KVASHUK used a 173.244.44 IP address and a test account used the same IP
10 address on the same day to purchase CSV.

11 37. Records obtained through the course of the investigation indicate that IP
12 addresses 173.244.44.19, 173.244.44.37, 173.244.44.58, and 173.244.44.89 are assigned
13 to the company London Trust Media, Inc. This company operates a virtual private
14 network (VPN) service that specializes in anonymity online through the website
15 www.privateinternetaccess.com. While I am continuing to investigate the 173.244.44 IP
16 addresses, I believe that all of the 173.244.44 IP addresses associated to this investigation
17 are controlled by London Trust Media, Inc.

18 38. Based on my training and experience, KVASHUK may have believed that
19 by using a VPN service specializing in online anonymity to commit the fraud, he could
20 disguise his involvement in the crimes.

21 39. Another IP address, 4.35.246.19, was also used to access the [REDACTED] and
22 [REDACTED] test accounts at least 24 times for purchases of over \$131,000 in CSV in
23 connection with the fraud. Although this IP address is still under investigation, it was
24 also used to access three Microsoft store accounts linked to KVASHUK. It was used at
25 least 54 times between October 24, 2017 and November 24, 2017 to access the pikimajdo
26 and xidijenizo accounts (the accounts used to order the graphics cards delivered to
27

28 ⁴ The kvashuk account is listed as KVASHUK's personal account on his resume.

1 "Grigory shikor" at KVASHUK's apartment complex) and used at least 21 times on
2 November 24, 2017 to access the the vokvas test account (the test account created by
3 KVASHUK).

4 40. A third IP address, 50.243.108.211, was used five times on December 12,
5 2017, to purchase approximately \$39,500 of CSV using the [REDACTED] test account. It
6 was also used 37 times on October 22, 2017 to access the vokvas, and xidijenizo
7 accounts.

8 41. The fact that all of the above IP addresses are linked to both KVASHUK
9 and the test accounts used to commit the fraud strongly suggests KVASHUK's
10 involvement in the crime.

11 42. KVASHUK is also linked to the [REDACTED], and [REDACTED] through a
12 technology known as "Fuzzy Device" identification. When a person uses a particular
13 device to access Microsoft's online store, that device leaves a digital trail known as a
14 "Fuzzy Device" identifier. According to Microsoft, although it is theoretically possible
15 for two devices to have the same Fuzzy Device ID, it is very unlikely. As a result, if
16 multiple logins are made from the same Fuzzy Device ID, there is a strong inference that
17 the same device (a particular computer, cell phone, etc.) was used to make all of those
18 logins. Between October 22, 2017 and November 26, 2017, Microsoft's records show
19 the same Fuzzy Device ID for logins to accounts believed to be associated with
20 KVASHUK (the vokvas, xidijenizo, and pikimajado accounts) as well as at least some
21 logins to the accounts that were primarily used to steal CSV (avestu and sfwe2eauto).
22 Similarly, Microsoft records show that the user who logged into all of those accounts
23 was, on at least some occasions, running the same version of the Linux operating system
24 and the same outdated version of the Mozilla Firefox browser – further evidence that a
25 single device logged into all of those accounts.

26 43. Based on my training and experience, I know that term "Device ID" is a
27 generic industry term for an identifier for an electronic device. Some devices have a
28 unique identifier specifically labeled as a "Device ID" by a hardware manufacturer.

AFFIDAVIT OF SA HERGERT
USAO#2018R01443

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE
5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

1 When one hardware manufacturer, website, government agency, or any other company
2 refers to the identification of, collection of, or use of a "Device ID", they are all generally
3 talking about a different identifier or mechanism for generating a Device ID that is
4 unique to that manufacturer or other entity. Device IDs are generally used to identify
5 multiple transactions conducted by the same device.

6 44. I also know that Device IDs are often created by collecting a very large
7 collection of not-so-unique browser and system components that a web-browser allows a
8 website to view/collect, such as operating system, web-browser, screen resolution, and
9 many other settings. If any of the settings used to calculate the Device ID change, the
10 Device ID will change. An individual with knowledge of Device IDs could disguise the
11 fact that they are conducting multiple transactions from the same device by changing
12 some of these settings. Additionally, Device IDs would change if the individual used
13 more than one device, or used virtual machines⁵ to simulate the use of more than one
14 device.

15 45. In total, Microsoft captured Fuzzy Device ID information on approximately
16 223 of the 1,554 purchases of CSV using the [REDACTED], and [REDACTED] accounts.⁶
17 Over the course of the scheme, a total of 14 different Fuzzy Device IDs were captured on
18 these 223 transactions. Most of the Fuzzy Device IDs were only used to purchase the
19 CSV for one day. This could be indicative of using multiple devices, or the use of virtual
20 machines. The first Fuzzy Device ID listed on the chart below -- bb92c484-876b-4d87-
21 adca-943b90a2d98e -- was used to access the vokvas, xidijenizo, and pikimajado
22 accounts between October 22 and 24, 2017, and was also used access the [REDACTED] and
23 [REDACTED] test accounts to make CSV purchases on November 26, 2017. This strongly
24

25
26 ⁵ A virtual machine is simulated computer that runs its own operating system that runs like an application on another
27 computer. The end user has a similar experience on a virtual machine as they would have if the operating system
28 were installed on its own device. Several virtual machines can be installed on a single computer, and can created in
a short period of time.

⁶ Fuzzy Device ID information was only captured for transactions conducted through the [REDACTED] and [REDACTED]
accounts.

suggests that the same device was used to access both accounts known to be linked to KVASHUK as well as the test accounts used to commit the fraud.

Device ID	Identified Occurrences	Date Range
bb92c484-876b-4d87-adca-943b90a2d98e	6	11/26/2017
58b04a06-d52c-481b-9050-34d1f5c64aab	20	12/2/2017 – 12/13/2017
3bab2d39-29f9-4332-bc96-3121a57d99cd	1	12/3/2017
c2313cdc-a005-421b-9fa9-159d2adbdf53	3	12/7/2017
aa29eee2-3f6d-45b4-9c01-cfa320b962b1	11	12/9/2017 – 12/12/2017
455010cd-e513-44c1-8fc0-f4495b0d7453	6	12/10/2017
6d2a6011-99b5-48be-b00c-130450b26272	12	12/14/2017
d117e690-0627-4624-912f-3a636457bf6d	19	12/15/2017
ec76885c-6718-4857-8ed9-8ea3f11ed30e	12	12/16/2017
84925c6b-035f-4138-9b41-b2dbbb13efce	10	12/17/2017
3b0d8c07-3656-4c4c-b938-8441c8c43716	17	12/19/2017 – 12/20/2017
21c35123-cccf-474f-ade4-8fd96984975d	79	12/22/2017 – 1/4/2018
486e5a23-b428-478c-99ed-7c25c8d76b25	25	1/12/2018
0424b94c-9e86-4abd-a9f4-bfce92f962a1	2	1/20/2018

Evidence Of Unexplained Wealth

46. Financial records show that KVASHUK had a large amount of unexplained income during the period of the CSV thefts. According to Microsoft, KVASHUK's annual salary was \$116,000. I have reviewed records for a checking account that KVASHUK had at Wells Fargo bank, ending in -5789. The earliest daily balance shown on the records was \$429.56 on July 29, 2016. The balance on the account remained under \$20,000 until late November of 2017, when large amounts of money from a cryptocurrency account in KVASHUK's name at Coinbase.com, began to flow into the -5789 account. On November 30, 2017, over \$14,000 was transferred to the -5789 account from Coinbase.com. On December 11, 2017, over \$4,600 was transferred from

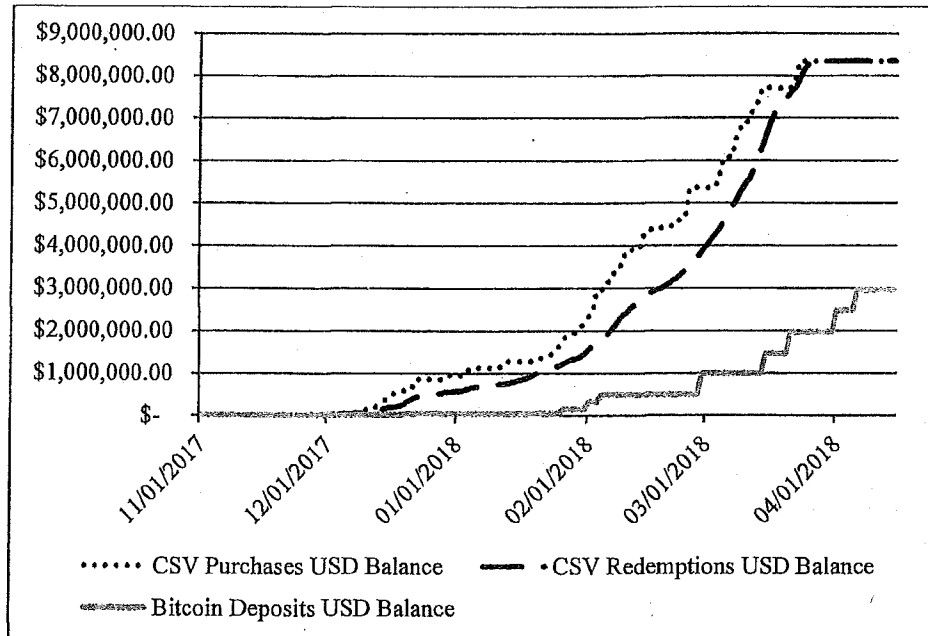
1 Coinbase.com to the -5789 account. On December 21, 2017, there was a transfer of over
2 \$29,000 from Coinbase.com to the -5789 account.

3 47. The suspicious transfers escalated dramatically in early 2018. For example,
4 on January 30th, February 2nd, and February 6th of 2018, there were transfers from
5 Coinbase of over \$98,000, \$177,000 and \$134,000, respectively. On a single day –
6 March 2, 2018 – over \$500,000 was transferred from Coinbase to the -5789 account.
7 Over \$1.4 million was transferred in total in March 2018, followed by over \$935,000 in
8 April.

9 48. All told, over \$2.8 million was transferred from Coinbase to the -5789
10 account between November 2017 and May 2018. The approximate timeframe of the
11 fraud was November 2017 through March 2018. Given these timeframes, and based on
12 my training and experience, it appears that KVASHUK had converted the proceeds of the
13 fraud into cryptocurrency, and then gradually converted the cryptocurrency in fiat
14 currency and transferring the proceeds to his Wells Fargo account.

15 49. Furthermore, in order to determine the source of the cryptocurrency
16 “bitcoin” in the Coinbase account, I have examined the bitcoin blockchain, a public
17 ledger of bitcoin transactions. I determined that the vast majority of the bitcoin deposited
18 into the Coinbase account originated from chipmixer.com. Chipmixer.com is a bitcoin
19 “mixing” service which appears to be located in Germany. A bitcoin mixing service
20 mixes potentially identifiable bitcoin with others, with the intent to obscure and conceal
21 the original source of the bitcoin. Based on my training and experience, the use of
22 chipmixer.com is further evidence of an attempt to conceal proceeds of the fraud. As part
23 of my investigation, I analyzed the value of bitcoin (in United States dollars) received
24 into KVASHUK’s Coinbase account and compared it to the purchase and redemptions of
25 CSV. I was able to determine that, while significantly lower, the value of the bitcoin
26 deposits to KVASHUK’s Coinbase account generally coincided with the value of the
27 purchased and redeemed CSV. The reason for the lower value could include KVASHUK
28

1 selling the CSV at a discount, bitcoin's general decline in value during early 2018, or that
 2 not all of the proceeds from this scheme have been identified.



15 50. KVASHUK has used his unexplained wealth to make significant purchases.
 16 In March of 2018, KVASHUK paid roughly \$162,000 for a Tesla vehicle. In May of
 17 2018, KVASHUK bought a lakeside home in Renton for roughly \$1.675 million, and
 18 apparently paid cash.⁷

20 **PROBABLE CAUSE REGARDING THE SUBJECT EMAIL ACCOUNTS**

21 51. As set forth above, there is probable cause to believe that evidence of the
 22 offenses of mail fraud, wire fraud and money laundering may be found in the SUBJECT
 23 EMAIL ACCOUNTS. The fraudulent scheme, by its nature, relied heavily upon email.
 24 With the exception of the kvashuk.volodymyr@gmail.com account, all of the SUBJECT
 25 EMAIL ACCOUNTS were used to purchase or redeem stolen digital currency or
 26 property. There is probable cause to search the kvashuk.volodymyr@gmail.com for a

28 ⁷ In bank account records, KVASHUK claims that the source of his wealth was family money.

1 variety of reasons. That account was accessed via IP addresses starting with 173.244.44,
2 which were also used primarily to commit the fraud, and thus any evidence linking
3 KVASHUK to that account also links him to the fraud. Furthermore, we have only
4 limited evidence as to how KVASHUK arranged to resell the CSV via online resellers,
5 what resellers he used, how the proceeds flowed back to him, and how he disposed of
6 those proceeds. From my training and experience, I know that KVASHUK may have
7 used email accounts, including the kvashuk.volodymyr@gmail.com account, to arrange
8 for the resale of CSV and the transfer of proceeds, as well as to otherwise carry out the
9 scheme.

10 52. Additionally, I know that Coinbase, and many other virtual currency related
11 entities often communicate with their customers via email. These communications may
12 be evidence of financial transactions conducted using the proceeds of the fraud, and
13 therefore be evidence of money laundering. Coinbase records specifically show
14 communication with the kvashuk.volodymyr@gmail.com email address.

15 **BACKGROUND REGARDING THE PROVIDERS' SERVICES**

16 53. In my training and experience, I have learned that the Providers provides a
17 variety of on-line services, including electronic mail ("e-mail") access, to the general
18 public. The Providers allow subscribers to obtain e-mail accounts at the domain names
19 set forth in this affidavit and the attachments.

20 54. Subscribers obtain an account by registering with the Providers. When
21 doing so, e-mail providers like the Providers ask the subscriber to provide certain
22 personal identifying information. This information can include the subscriber's full
23 name, physical address, telephone numbers and other identifiers, alternative e-mail
24 addresses, and, for paying subscribers, means and source of payment (including any
25 credit or bank account number). In my training and experience, such information may
26 constitute evidence of the crimes under investigation because the information can be used
27 to identify the account's user or users, and to help establish who has dominion and
28 control over the account.

1 55. E-mail providers typically retain certain transactional information about the
2 creation and use of each account on their systems. This information can include the date
3 on which the account was created, the length of service, records of log-in (i.e., session)
4 times and durations, the types of service utilized, the status of the account (including
5 whether the account is inactive or closed), the methods used to connect to the account
6 (such as logging into the account via a Provider's website), and other log files that reflect
7 usage of the account. In addition, e-mail providers often have records of the Internet
8 Protocol address ("IP address") used to register the account and the IP addresses
9 associated with particular logins to the account. Because every device that connects to
10 the Internet must use an IP address, IP address information can help to identify which
11 computers or other devices were used to access the e-mail account, which can help
12 establish the individual or individuals who had dominion and control over the account.

13 56. In general, an e-mail that is sent to the Providers' subscribers is stored in
14 the subscriber's "mail box" on the Providers' servers until the subscriber deletes the e-
15 mail. If the subscriber does not delete the message, the message can remain on the
16 Providers' servers indefinitely. Even if the subscriber deletes the e-mail, it may continue
17 to be available on the Providers' servers for a certain period of time.

18 57. When the subscriber sends an e-mail, it is initiated at the user's computer,
19 transferred via the Internet to the Providers' servers, and then transmitted to its end
20 destination. The Providers often maintains a copy of the e-mail sent. Unless the sender
21 of the e-mail specifically deletes the e-mail from the Providers' server, the e-mail can
22 remain on the system indefinitely. Even if the sender deletes the e-mail, it may continue
23 to be available on the Providers' servers for a certain period of time.

24 58. A sent or received e-mail typically includes the content of the message,
25 source and destination addresses, the date and time at which the e-mail was sent, and the
26 size and length of the e-mail. If an e-mail user writes a draft message but does not send
27 it, that message may also be saved by the Providers but may not include all of these
28 categories of data.

1 59. An Outlook.com subscriber can also store files, including address books,
2 contact lists, calendar data, photographs, and other files, on servers maintained and/or
3 owned by Microsoft. I know based on my training and experience and my review of
4 Microsoft Outlook.com's services, that Outlook.com provides users with access to a
5 "People" file in which they may store contact information including names, addresses, e-
6 mail address, telephone numbers, birthdates, job titles, and other notes. Outlook.com also
7 provides users access to a "Calendar" file that may include notes of events and schedules.
8 In addition, Outlook.com provides users with access to a "OneDrive" which provides
9 users with cloud based storage of files including photographs and other documents such
10 as Word processing documents or spreadsheets. Outlook.com allows users to share their
11 OneDrive content with others or the public depending on the settings selected by the
12 account holder. In my training and experience, evidence of who was using an e-mail
13 account may be found in address books, calendars, photographs and other documents
14 stored in relation to the account.

15 60. A subscriber to a Google Gmail account can also store files, including
16 address books, contact lists, calendar data, photographs and other files, on servers
17 maintained and/or owned by Google. For example, Google offers users a calendar
18 service that users may utilize to organize their schedule and share events with others.
19 Google also offers users a service called Google Drive that may be used to store data and
20 documents. The Google Drive service may be used to store documents including
21 spreadsheets, written documents (such as Word or Word Perfect) and other documents
22 that could be used to manage a website. Google Drive allows users to share their
23 documents with others or the public depending on the settings selected by the account
24 holder. Google also provides its users with access to the photo storage service "Picasa."
25 Picasa can be used to create photo albums, store photographs, and share photographs with
26 others. Another Google service called "You Tube" allows users to view, store and share
27 videos. Google also provides a service called "Google Analytics. Google Analytics is a
28 Google service that monitors website traffic and provides subscribers with data relating to

1 how much traffic is visiting the subscriber's website, which sections of the subscriber's
2 website users are visiting, how long users are staying on particular sections of the site,
3 and the geographical source of users visiting the website, among other things.

4 61. The additional services provided by Google and Microsoft, referenced in
5 the paragraphs above, are relevant to establish who had dominion or control over the
6 various email accounts. Furthermore, the content – such as calendar entries, stored
7 documents, spreadsheets, and other material – may be evidence of the actual fraud, which
8 was data-intensive and would have required the transmission and storage of various types
9 of data.

10 62. In some cases, e-mail account users will communicate directly with an e-
11 mail service provider about issues relating to the account, such as technical problems,
12 billing inquiries, or complaints from other users. E-mail providers typically retain
13 records about such communications, including records of contacts between the user and
14 the provider's support services, as well records of any actions taken by the provider or
15 user as a result of the communications. In my training and experience, such information
16 may constitute evidence of the crimes under investigation because the information can be
17 used to identify the account's user or users.

18 **PAST EFFORTS TO OBTAIN THIS EVIDENCE**

19 63. This evidence has not been previously available to me or other agents, apart
20 from subscriber information records and non-content information obtained via an 18
21 U.S.C. § 2703(d) order.

22 **PROTOCOL FOR SORTING SEIZABLE**

23 **ELECTRONICALLY STORED INFORMATION**

24 64. In order to ensure that agents are limited in their search only to the e-mail
25 account specifically sought (and any attachments, stored instant messages, stored voice
26 messages, and photographs associated therewith); in order to protect the privacy interests
27 of other third parties who have accounts at the Providers; and in order to minimize
28 disruptions to normal business operations of the Providers; this application seeks

1 authorization to permit agents and employees of the Providers to assist in the execution of
2 the warrants, as follows: (See: Title 18, United States Code, Section 2703(g)).

3 65. The search warrants will be presented to the Providers, with direction that
4 they identify and isolate the e-mail accounts and associated records described in Section I
5 of Attachments B and B-1.

6 66. The Providers will also be directed to create an exact duplicate in electronic
7 form of the e-mail accounts and records specified in Section I of Attachments B and B-1,
8 including an exact duplicate of the content of all e-mail messages stored in the specified
9 e-mail account.

10 67. The Providers shall then provide exact digital copies of the content of the
11 subject e-mail accounts, as well as all other records associated with the account, to me, or
12 to any authorized federal law enforcement agent assigned to this case. Once the digital
13 copies have been received from the Providers, that copy will, in turn, be forensically
14 imaged and only that image will be reviewed and analyzed to identify communications
15 and other data subject to seizure pursuant to Section II of Attachments B and B-1. The
16 original digital copies will be sealed and maintained to establish authenticity, if
17 necessary.

18 68. I, and/or other agents of IRS-CI, the United States Secret Service (USSS),
19 or other federal law enforcement agency assigned to this case will thereafter review the
20 forensic images, and identify from among that content those items that come within the
21 items identified in Section II to Attachments B and B-1, for seizure. I, and/or other
22 agents identified above will then copy those items identified for seizure to separate media
23 for future use in the investigation and prosecution. The forensic copy of the complete
24 content of the e-mail accounts will also then be sealed and retained by IRS-CI and/or
25 USSS, and will not be unsealed absent authorization of a Magistrate Judge of this Court,
26 except for the purpose of duplication of the entire image in order to provide it, as
27 discovery, to a charged defendant.
28

1 69. Analyzing the data contained in the forensic image may require special
2 technical skills, equipment, and software. It could also be very time-consuming.
3 Searching by keywords, for example, can yield thousands of "hits," each of which must
4 then be reviewed in context by the examiner to determine whether the data is within the
5 scope of the warrant. Merely finding a relevant "hit" does not end the review process.
6 Keywords used originally need to be modified continuously, based on interim results.
7 Certain file formats, moreover, do not lend themselves to keyword searches, as keywords
8 search text, and many common electronic mail, database, and spreadsheet applications,
9 (which may be attached to e-mail,) do not store data as searchable text. The data is
10 saved, instead, in proprietary non-text format. And, as the volume of storage allotted by
11 service providers increases, the time it takes to properly analyze recovered data increases,
12 as well. Consistent with the foregoing, searching the recovered data for the information
13 subject to seizure pursuant to this warrant may require a range of data analysis techniques
14 and may take weeks or even months.

15 70. Based upon my experience and training, and the experience and training of
16 other agents with whom I have communicated, it is necessary to review and seize all
17 electronic mails, chat logs and documents, that identify any users of the subject account
18 and any electronic mails sent or received in temporal proximity to incriminating e-mails
19 that provide context to the incriminating communications.

20 71. All forensic analysis of the image data will employ only those search
21 protocols and methodologies reasonably designed to identify and seize the items
22 identified in Section II of Attachments B and B-1 to the warrant.

23 72. Records and files that could otherwise be obtained by subpoena shall
24 remain available, in their entirety, to investigating agents and prosecutors for the duration
25 of the investigation and prosecution. These include the name and address of the
26 subscriber to or customer of the service; local and long distance telephone connection
27 records; records of session times and durations; length of service and types of services
28 utilized; telephone or instrument number or other subscriber number or identity,

1 including any temporarily assigned network address; and means and source of payment,
2 including any credit card and bank account numbers.

3 73. If in the course of their efforts to identify and segregate evidence of the
4 items specified in Section II to Attachments B and B-1, law enforcement agents or
5 analysts discover items outside of the scope of the warrant that are evidence of other
6 crimes, that data/evidence will not be used in any way unless it is first presented to a
7 Magistrate Judge of this District and a new warrant is obtained to seize that data, and/or
8 to search for other evidence related to it. In the event a new warrant is authorized, the
9 government may make use of the data then seized in any lawful manner.

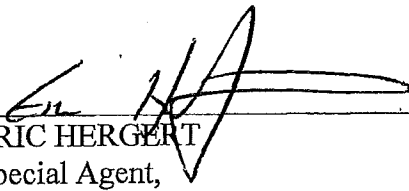
10 **REQUEST FOR NON-DISCLOSURE AND SEALING**

11 74. The government requests, pursuant to the preclusion of notice provisions of
12 Title 18, United States Code, Section 2705(b), that the Providers be ordered not to notify
13 any person (including the subscriber or customer to which the materials relate) of the
14 existence of this warrant for such period as the Court deems appropriate. The
15 government submits that such an order is justified because notification of the existence of
16 this Order would seriously jeopardize the ongoing investigation. Such a disclosure would
17 give the subscriber an opportunity to destroy evidence, change patterns of behavior,
18 notify confederates, or flee or continue his flight from prosecution.

19 75. It is further respectfully requested that this Court issue an order sealing,
20 until further order of the Court, all papers submitted in support of this application,
21 including the application and search warrant. This is an ongoing investigation, and the
22 target did not know the details of what investigators have learned and what evidence
23 has been gathered. Premature disclosure of the contents of this affidavit and related
24 documents may have a significant and negative impact on the continuing investigation
25 and may severely jeopardize its effectiveness by resulting in the flight of the target, the
26 destruction of evidence, or the intimidation or influencing of witnesses.

CONCLUSION

76. Based on the forgoing, I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated," per 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Accordingly, by this Affidavit and Warrant I seek authority for the government to search all of the items specified in Section I, Attachments B and B-1 (attached hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of the data, documents and records that are identified in Section II to those same Attachments.



ERIC HERGERT
Special Agent,
Internal Revenue Service

SUBSCRIBED AND SWORN before me this 29 day of April, 2019.



BRIAN A. TSUCHIDA
Chief United States Magistrate Judge

ATTACHMENT A

Accounts to be Searched

The electronically stored data, information, and communications contained in, related to, and associated with the following email accounts, which are located at premises owned, maintained, controlled, or operated by Microsoft Corporation, an email provider headquartered at 1 Microsoft Way, Redmond, Washington 98052:

safirion@outlook.com;

[REDACTED]@outlook.com;

[REDACTED]@outlook.com;

mstest_v-vokvas@outlook.com; and

[REDACTED]@outlook.com

ATTACHMENT A-1

Account to be Searched

The electronically stored data, information, and communications contained in, related to, and associated with the following email account, as well as all other email accounts linked to the identified accounts through the same phone number, alternate email address, registration IP address, device ID information, or internet cookies, as well as all other subscriber and log records associated with the accounts, which are located at premises owned, maintained, controlled, or operated by Google, Inc., an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043:

kvashuk.volodymyr@gmail.com.

Google, Inc., shall also produce any and all material preserved pursuant to the preservation request sent on February 1, 2019 (Google reference number 2307267).

ATTACHMENT B

I. Section I - Information to be disclosed by Microsoft Corporation, for search:

For the time period from January 1, 2016, to the present, to the extent that the information described in Attachment A is within the possession, custody, or control of Microsoft Corporation ("Microsoft"), including any e-mails, records, files, logs, or information that has been deleted but is still available to Microsoft, Microsoft is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, forwarding email addresses, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records pertaining to communications between Microsoft and any person regarding the account, including contacts with support services and records of actions taken.
- e. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- f. All subscriber records associated with the specified account including lists of all related accounts, any contact lists, and content and/or preserved data;
- g. All records available regarding the location of the user of the account, including information obtained from IP addresses, GPS, wifi access points, or cell towers;

- 1
- 2 h. All records regarding device-specific information for devices used to access the
- 3 accounts, including hardware model, operating system, unique device identifiers,
- 4 and mobile network information, including phone numbers;
- 5
- 6 i. Records of any other accounts associated with the account through common
- 7 cookies, device identifiers, email addresses, or phone numbers;
- 8
- 9 j. Internet browsing and search history information for the account; and
- 10
- 11 k. subscriber information and log records regarding any other email accounts linked
- 12 to the identified accounts through the same phone number, alternate email address,
- 13 registration IP address, device ID information, or internet cookies.
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28

1 **II. Section II - Information to be seized by the government**

2 All information described above in Section I that constitutes fruits, contraband,
3 evidence and instrumentalities of violations of Mail Fraud, in violation of Title 18,
4 United States Code, Section 1341, Wire Fraud, in violation of Title 18, United States
5 Code, Section 1343, and Money Laundering, in violation of Title 18, United States Code,
6 Sections 1956(a)(1) and 1957, including, for the account or identifier listed on
7 Attachment A, information pertaining to the following matters:

- 8
- 9 a. Communications or material related to the purchase or attempted online purchase
10 of any products or services from Microsoft Corporation, including but not limited
11 to purchases of currency stored value, digital currency, gift cards, movies, video or
12 graphics cards, or subscriptions;
- 13 b. Communications, or material related to the actual or attempted transfer, resale, or
14 redemption of Microsoft currency stored value, digital currency, gift cards, or
15 subscriptions;
- 16 c. Communications or material related to online resellers;
- 17 d. Communications or material related the possible transfer or disposition of the
18 proceeds of the fraud, including but not limited: to accounts at banks or other
19 financial institutions; financial transactions or transfers; the purchase, transfer or
20 sale of cryptocurrency; the use of the proceeds of the fraud to buy real property,
21 vehicles, or goods or services; and any explanations, reports, or other information
22 regarding the amount and sources of funds or other income;
- 23 e. Communications or material related to "Grigor Shikor" or "Grigory Kvashuk";
- 24 f. All messages, documents, and profile information, attachments, or other data that
25 serves to identify any persons who use or access the account specified, or who
26 exercise in any way any dominion or control over the specified account;
- 27 g. Any address lists or buddy/contact lists associated with the specified account;
- 28 h. All messages, documents and profile information, attachments, or other data that
 otherwise constitutes evidence, fruits, or instrumentalities of violations of Mail
 Fraud, in violation of Title 18, United States Code, Section 1341, Wire Fraud, in

1 violation of Title 18, United States Code, Section 1343, and Money Laundering, in
2 violation of Title 18, United States Code, Sections 1956(a)(1) and 1957.

- 3 i. All subscriber associated with the specified account, including name, address,
4 local and long distance telephone connection records, or records of session times
5 and durations, length of service (including start date) and types of service utilized,
6 telephone or instrument number or other subscriber number or identity, including
7 any temporarily assigned network address, and means and source of payment for
8 such service) including any credit card or bank account number;
- 9 j. Any records of communications between the email service provider, and any
10 person about issues relating to the account, such as technical problems, billing
11 inquiries, or complaints from other users about the specified account. This to
12 include records of contacts between the subscriber and the provider's support
13 services, as well as records of any actions taken by the provider or subscriber as a
14 result of the communications.
15
16
17
18
19
20
21
22
23
24
25
26
27
28

AFFIDAVIT OF SA HERGERT
USAO#2018R01443

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE
5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-1

I. Section I - Information to be disclosed by Google, Inc., for search:

For the time period from the time period from January 1, 2016, to the present, to the extent that the information described in Attachment A-1 is within the possession, custody, or control of Google, Inc. ("Google"), including any e-mails, records, files, logs, or information that has been deleted but is still available to Google, Google is required to disclose the following information to the government for each account or identifier listed in Attachment A-1:

- a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, forwarding email addresses, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records pertaining to communications between Microsoft and any person regarding the account, including contacts with support services and records of actions taken.
- e. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- f. All subscriber records associated with the specified account including lists of all related accounts, any contact lists, and content and/or preserved data;
- g. All records available regarding the location of the user of the account, including information obtained from IP addresses, GPS, wifi access points, or cell towers;

- 1
- 2 h. All records regarding device-specific information for devices used to access the
- 3 accounts, including hardware model, operating system, unique device identifiers,
- 4 and mobile network information, including phone numbers;
- 5 i. Records of any other accounts associated with the account through common
- 6 cookies, device identifiers, email addresses, or phone numbers;
- 7 j. Internet browsing and search history information for the account; and
- 8 k. Subscriber information and log records regarding any other email accounts linked
- 9 to the identified accounts through the same phone number, alternate email address,
- 10 registration IP address, device ID information, or internet cookies.
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28

AFFIDAVIT OF SA HERGERT
USAO#2018R01443

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE
5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

II. Section II - Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Mail Fraud, in violation of Title 18, United States Code, Section 1341, Wire Fraud, in violation of Title 18, United States Code, Section 1343, and Money Laundering, in violation of Title 18, United States Code, Sections 1956(a)(1) and 1957, including, for the account or identifier listed on Attachment A-1, information pertaining to the following matters:

- a. Communications or material related to the purchase or attempted online purchase of any products or services from Microsoft Corporation, including but not limited to purchases of currency stored value, digital currency, gift cards, movies, video or graphics cards, or subscriptions;
- b. Communications, or material related to the actual or attempted transfer, resale, or redemption of Microsoft currency stored value, digital currency, gift cards, or subscriptions;
- c. Communications or material related to online resellers;
- d. Communications or material related the possible transfer or disposition of the proceeds of the fraud, including but not limited: to accounts at banks or other financial institutions; financial transactions or transfers; the purchase, transfer or sale of cryptocurrency; the use of the proceeds of the fraud to buy real property, vehicles, or goods or services; and any explanations, reports, or other information regarding the amount and sources of funds or other income;
- e. Communications or material related to "Grigor Shikor" or "Grigory Kvashuk";
- f. All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account;
- g. Any address lists or buddy/contact lists associated with the specified account;
- h. All messages, documents and profile information, attachments, or other data that otherwise constitutes evidence, fruits, or instrumentalities of violations of Mail Fraud, in violation of Title 18, United States Code, Section 1341, Wire Fraud, in

1 violation of Title 18, United States Code, Section 1343, and Money Laundering, in
2 violation of Title 18, United States Code, Sections 1956(a)(1) and 1957.

- 3 i. All subscriber associated with the specified account, including name, address,
4 local and long distance telephone connection records, or records of session times
5 and durations, length of service (including start date) and types of service utilized,
6 telephone or instrument number or other subscriber number or identity, including
7 any temporarily assigned network address, and means and source of payment for
8 such service) including any credit card or bank account number;
- 9 j. Any records of communications between the email service provider, and any
10 person about issues relating to the account, such as technical problems, billing
11 inquiries, or complaints from other users about the specified account. This to
12 include records of contacts between the subscriber and the provider's support
13 services, as well as records of any actions taken by the provider or subscriber as a
14 result of the communications.
- 15
16
17
18
19
20
21
22
23
24
25
26
27
28